AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A direct memory access memory corruption detection system embodied on a computer readable medium comprising the following computer executable components:

an access data store that stores access information associated with memory, the access data store comprising an access table, the access table comprising a source identifier field, a memory address field and an access attribute field, the access attribute field distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory address range associated with the access attribute identified in the source identifier field and memory address field; and.

a memory controller that employs the access information to determine whether a requested direct memory access is permitted and rejects the requested direct memory access if it is not permitted and allows the requested direct memory access if it is permitted.

2. (Previously Presented) The direct memory access memory corruption detection system of claim 1, the access information comprising a direct memory access request.

3. (Previously Presented) The direct memory access memory corruption detection system of claim 2, the direct memory access request comprising a transaction type.

4. (Previously Presented) The direct memory access memory corruption detection system of claim 1, the direct memory access request comprising a source identifier.

5. (Original) The direct memory access memory corruption detection system of claim 4, the source identifier being associated with a device.

6. (Cancelled).

7. (Original) The direct memory access memory corruption detection system of claim 1, the access information comprising at least one permitted memory address.

8. (Original) The direct memory access memory corruption detection system of claim 1, the access information comprising at least one disallowed memory address.

9. (Original) The direct memory access memory corruption detection system of claim 1, the request comprising a read action or a write action.

10. (Previously Presented) The direct memory access memory corruption detection system of claim 1, the request comprising a peripheral component interconnect express bus transaction.

11. (Previously Presented) The direct memory access memory corruption detection system of claim 1, the memory controller coupled to a device through a peripheral component interconnect express bus, the device providing the request.

12. (Original) The direct memory access memory corruption detection system of claim 1, the memory controller further providing error information, if the requested direct memory access is not permitted.

13. (Original) The direct memory access memory corruption detection system of claim 12, the error information comprising source information associated with the requested direct memory access.

14. (Currently Amended) A direct memory access memory corruption detection system embodied on a computer readable medium comprising the following computer executable components:

a memory controller that includes an access data store comprising an access table, the access table comprising a source identifier field, a memory address field and an access attribute field, the access attribute field contains an access attribute that distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory address range associated with the access attribute identified in the source identifier field and memory address field ~~an access table store that stores access information associated with memory, the access information comprising at least one source identifier, at least one memory address and at least one access attribute, an access attribute distinguishes from amongst read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source and memory range identified by a source identifier associated with the access attribute and a memory address associated with the access attribute~~, wherein the access attribute contains data indicating read when the source identified by the source identifier associated with the access attribute is only permitted to read the memory address range associated with the access attribute, wherein the access attribute contains data indicating write when the source identified by the source identifier associated with the access attribute is only permitted to write to the memory address range associated with the access attribute, wherein the access attribute contains data indicating read and write when the source identified by the source identifier associated with the access attribute is permitted to read and write to the memory address range associated with the access attribute, wherein the access attribute contains data indicating no access when the source identified by the source identifier associated with the access attribute is not permitted access to the memory address range associated with the access attribute, the memory controller employs the access information to determine whether a requested direct memory access is permitted and rejects the requested direct memory access if it is not permitted and allows the requested direct memory access if it is permitted; and,

a device driver that programs a device for a direct memory access operation, and, provides the access information to the memory controller *via* a direct memory access application interface.

15. (Previously Presented) The direct memory access memory corruption detection system of claim 14, the device driver providing access information comprising a range of physical memory, a source identifier, and, an access attribute.

16. (Previously Presented) The direct memory access memory corruption detection system of claim 14, the request comprising a peripheral component interconnect express bus transaction.

17. (Currently Amended) A method that facilitates detection of direct memory access memory corruption comprising:

receiving a request for a direct memory access transaction, the request comprising a source identifier, at least one memory address, and an ~~transaction~~ access attribute; and,

determining whether the request is permitted based, at least in part on, stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute, an access attribute distinguishes between read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source associated with the access attribute and memory range associated with the access attribute identified by the at least one source identifier and at least one memory address range; and

rejecting the requested direct memory access if it is not permitted and allowing the direct memory access if it is permitted.

18. (Cancelled)

19. (Currently Amended) The method of claim 17, storing access information in a access data store, the access information comprising at least one source identifier, at least one memory address range and at least one an access attribute.

20. (Original) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 17.

21. (Currently Amended) A data packet transmitted between two or more components embodied on a computer readable medium that facilitates detection of direct memory access memory corruption, the data packet comprising:

a data field comprising a corrected platform error event, the corrected platform error event being based, at least in part, upon a determination that a requested direct memory access is not permitted, the determination being based, at least in part, upon access information stored in an access table and the requested direct memory access, the access information comprising at least one source identifier, at least one memory address range and at least one access attribute, the at least one access attribute distinguishes from amongst read, read and write, write, and no access to indicate read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute.

22. (Currently Amended) A direct memory access memory corruption detection system embodied on a computer readable medium comprising:

means for storing access information associated with memory;

means for receiving a request for a direct memory access;

means for determining whether a requested direct memory access is permitted based, at least in part, upon the stored access information and the request, the stored access information comprising at least one source identifier, at least one memory address range and at least one access attribute, the at least one access attribute distinguishes between read, read and write, write, and no access to indicate one of read, read and write, write, or no access for a combination of source and memory address range identified by the at least one source identifier and at least one memory address range associated with the at least one access attribute; and,

means for rejecting the requested direct memory access if it is not permitted and allowing the direct memory access if it is permitted.